Journal of Information Security and Applications 40 (2018) 92–102

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A color image steganography in hybrid FRT–DWT domain

Rohit Thanki [a,*], Surekha Borra [b]

[a] C. U. Shah University, Wadhwan City, India
[b] K. S. Institute of Technology, Bangalore, India

ARTICLE INFO

Article history:

Keywords:
Color image
Discrete Wavelet Transform (DWT)
Embedding capacity
Finite Ridgelet Transform (FRT)
Security
Steganography

ABSTRACT

In this paper, a color image steganography technique based on Finite Ridgelet Transform (FRT) and Discrete Wavelet Transform (DWT) is proposed. The FRT is applied on the cover color image to get Ridgelet coefficients of each color channel of cover color image and a single level DWT is applied to get different wavelet coefficients, which are further modified by encrypted channel values of secret color image to get stego color image. In the proposed method, Arnold scrambling is used to encrypt channels of secret color image. The proposed technique is tested for its effectiveness on various types of standard color images and the results showed improved imperceptibility of the stego image compared to the existing technique. Further, the embedding capacity of the proposed technique is high.

1. Introduction

Since last few years, color images are used in many social media like Facebook, WhatsApp, and Instagram. These images are transferred from one computer or network or server to another using open networks such as the internet, wireless network etc., wherein they can undergo many manipulations and attacks [1–4]. So a strong communication technique is required for secure transmission of color images over any open access medium. Many steganographic and watermarking techniques are presented in the literature for this purpose. Since the year 2000, researchers developed and implemented various techniques in spatial domain and transform domains such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and so on [1–4] to hide binary logos/color images into the color cover images [5–19].

Phadikar et al. (2007) [5] proposed wavelet transform based blind watermarking technique for security of color images. In this technique, binary logo is embedded into the wavelet subbands of the Region of Interest (ROI) of the color image. Anitha and Pandian (2010) [6] proposed Self-Organizing Feature Map (SOFM) Vector Quantizer (VQ) based watermarking technique for the security of color images. In this technique, binary logo bits are inserted into the selected VQ encoded block of color image. Gunjal (2011) [7] proposed wavelet transform and Arnold scrambling based blind watermarking technique for the security of color images. In this technique, first, the color image is converted in YUV color space. Then third level HL subband coefficients of V channel of color image are modified by the PN sequence according to the scrambled watermark bits generated from Arnold scrambling. Dey et al. (2012) [8] proposed Discrete Wavelet Transform (DWT), spread spectrum, and Harris corner detection based watermarking techniques for security of color medical images. In this technique, first, Harris corner detection is applied to medical images to get its ROI. Then wavelet transform is applied to the Green channel of ROI of medical image to get wavelet coefficients. The HH subband of Green channel of ROI of medical image is modified by the PN sequence according to the watermark bits to get the watermarked color medical image.

Eswaraiah and Reddy (2012) [9] proposed DWT and Discrete Cosine Transform (DCT) based watermarking technique for security of color images. In this technique, first, a two-level DWT is applied to blue channel of color image to get wavelet coefficients. The DCT is applied to LH2 subband coefficients to get its DCT coefficients. The DCT coefficients of blue channel of color image are modified by DCT coefficients of binary logo. Gunjal and Mail [10] proposed Singular Value Decomposition (SVD) and DWT based watermarking technique for security of color images. In this technique, first color image is converted into YUV color space. The scrambled watermark bits are inserted into singular values of third level HL subband coefficients of Y components using a gain factor. The scrambled watermark bits are generated using Arnold scrambling technique. Liu et al. (2012) [11] proposed DWT based watermarking technique for security of color pathological sensed image.

Nasir and Abdurrman (2013) [12] proposed a blind watermarking technique using DWT for color image protection. In this technique, watermark bits are inserted by modifying two largest DWT coefficients in non-overlapping blocks of subband coefficients such as LH, HL, and HH of Y component or blue channel of color im-

* Corresponding author.
E-mail addresses: rohitthanki9@gmail.com (R. Thanki), borrasurekha@gmail.com (S. Borra).

https://doi.org/10.1016/j.jisa.2018.03.004
2214-2126/

age. Yan and Yang (2013) [13] proposed Hadamard Transform (HT) and DWT based watermarking technique for security of color images. In this technique, first, G channel values of color image are partitioned into non-overlapping blocks. The HT is applied on it to get its HT coefficients. The single level DWT is applied to DC values of HT coefficients to obtain different wavelet subbands. The coefficients of LL subband are modified by encrypted watermark bits. The encrypted watermark bits are generated using XOR-based encryption method. ElGamal et al. (2013) [14] proposed DCT and DWT based blind watermarking technique for security of color images. In this technique, first, color image is converted into YUV color space. The Y component of image is partitioned into non-overlapping blocks and DCT is applied on it to get its DCT coefficients. A single level DWT is applied on these DCT coefficients, and then LL wavelet subband coefficients are modified by two PN sequences according to watermark bits.

Shi et al. (2014) [15] proposed Chebyshev chaotic map based encryption and SVD based blind watermarking technique for security of color images. In this technique, first, Chebyshev chaotic map based encryption is applied to watermark bits to get encrypted watermark bits. The singular values of encrypted watermark bits are then inserted into the singular value of blue channel of color image to get watermarked color image. Deshmukh et al. (2014) [16] proposed Redundant DWT and DCT based blind watermarking technique for security of color images. In this technique, DCT coefficients of second level HH wavelet subband coefficients of blue channel of color image are modified according to watermark bits to get watermarked color image. Rahman and Rabbi (2015) [17] proposed DWT and SVD based watermarking technique for security of color images. In this technique, singular values of HL subband wavelet coefficients of Red channel of color image are modified by watermark bits to get watermarked color image. Shakunthala et al. (2017) [18] proposed DWT, SVD, and Arnold scrambling based watermarking technique for security of color images. In this technique, first, color image is converted into YCbCr color space. The singular values of 4th level HL subband wavelet coefficients of Cb channel of color image are modified by scrambled watermark bits which are generated using Arnold scrambling technique. Abraham and Paul (2017) [19] proposed spatial domain watermarking technique for security of color images. In this technique, first a color image is decomposed into R–G–B channel, and then each channel is partitioned into non-overlapping blocks. A region for watermark bits embedding in the blocks of R channel is found using Simple Region Image Detection (SRID) approach. Finally, watermark bits are inserted into detected region of R channel of color image to get watermarked color image.

Many steganography techniques are also proposed and implemented by researchers for insertion of secret color image into the color cover image [20–28]. Chou and Wu (2003) [20] proposed quantization based steganography technique for color image protection. In this technique, color cover image and secret color image are converted into YUV color space. The value of Y–U–V channel of secret color image is embedded into corresponding channel of color cover image to get stego color image. Biswas et al. (2011) gave comparison of different steganography techniques [21,43–45] such as Least Significant Bit (LSB) substitution, Visual cryptography based technique, and Randomized LSB–MSB based techniques for color images. Su et al. (2012) [22] proposed Schur decomposition based steganography technique for color image protection. In this technique, first color cover image is decomposed into R–G–B channels. Each channel of cover image is then partitioned into 4×4 non-overlapping blocks and Schur decomposition is applied to it to get U matrix value for each channel. The values of U (2, 1) and U (3, 1) of U matrix of each channel of color cover image are modified according to the corresponding channel values of encrypted secret color image to get stego color image. The encrypted secret color image is generated using hash permutation. Su et al. (2013) [23] also proposed a two-level DCT based steganography technique for color image protection. In this technique, color cover image is divided into R, G and B channels, and every channel is divided into 8×8 blocks. The block-wise DCT is applied on blocks followed by second level DCT application on 4×4 upper left low frequency DCT coefficients. One secret bit is embedded into DC coefficients and seven secret bits are embedded into AC coefficients using binary logic operation. This process is repeated for each channel of cover color image for hiding the corresponding bits of each channel of the secret color image. Kumar and Anuradha (2014) [24] proposed DWT based steganography technique for color image protection. In this technique, wavelet coefficients of each channel of secret color image are inserted into wavelet coefficients of each corresponding channel of cover color image to get stego color image.

Vaishnavi and Subashini (2015) [25] proposed SVD based steganography technique for color image protection. In this technique, singular values of each channel of cover color image are modified by singular values of each corresponding channel of the encrypted secret color image, generated using Arnold scrambling technique. Rahman and Rabbi (2015) [26] proposed SVD and DWT based steganography technique for color image protection. In this technique, singular values of 4th level LL subband wavelet coefficients of each channel of cover color image are modified by singular values of each corresponding channel of secret color image. Freitas et al. (2016) [27] proposed halftone based steganography technique for color image protection. In this technique, secret color image is inserted into halftone generated cover color image. Jia et al. (2017) [28] proposed DWT and QR decomposition based steganography technique for color image protection. In this technique, the cover color image and secret color image are first decomposed into R, G, and B channels. DWT is then applied to cover color image to get wavelet coefficients of each channel of cover color image. These coefficients are divided into 4×4 non-overlapping blocks and then QR decomposition is applied on it to get R matrix. The R matrices of each channel of cover color image are modified by encrypting each channel values of secret color image. The encrypted secret color image is generated using Arnold transformation. The embedding capacity of this technique is 0.03125.

It is observed that all the above existing techniques are implemented in the transform domain using various image processing transforms such as DCT, DWT, and SVD for secret color image protection and have a limitation of less imperceptibility and less embedding capacity. This leaves a scope for development of novel techniques for securing color images. In this paper, a novel hybrid domain based color image steganography technique is proposed. The steganography technique is based on Finite Ridgelet Transform (FRT) [29–36], DWT and Arnold scrambling [28]. The logic behind using Finite Ridgelet Transform (FRT) in proposed technique is that there are less steganography or watermarking techniques are proposed using FRT for security of color images and improves the embedding capacity of steganography technique which is less in many existing techniques. The FRT also overcomes reconstruction limitation of DWT.

In the proposed technique, at first, cover color image is decomposed into its R, G, and B channels. Then FRT is applied on each channel of cover color image to get its ridgelet coefficients. Later, single level DWT is applied on ridgelet coefficients to get different wavelet subbands like LL, LH, HL, and HH for each channel of cover color image. The secret color image is also decomposed into its R, G, and B channels. The Arnold scrambling is applied to each channel to get encrypted channels of secret color image. Later, values of LL subband coefficients of each channel of cover color image are modified by corresponding values of each channel of encrypted secret color image according to insertion factor. Finally, inverse single

level DWT (IDWT) and inverse FRT are applied on modified coefficients to get stego color image. The secret color image extraction is performed using reverse process of watermark insertion.

In the proposed technique, the reason behind using FRT combination with DWT is that it improves the embedding capacity when compared to the techniques that uses only DWT [28]. When single level DWT is applied to an image of size $M \times N$, then it decomposes image into its subbands with wavelet coefficients of size $M/2 \times N/2$. This indicates that the technique that uses one subband of DWT can embed a watermark of maximum size as $M/2 \times N/2$. Thus, maximum embedding capacity of technique using DWT is 2 bits per pixel (bpp) for grayscale image as well as color image. On the other hand if a single level FRT is applied to an image of size $M \times N$, it decomposes into ridgelet coefficients of size $2M \times 2N$. Further application of single level DWT on these ridgelet coefficients results in $M \times N$ hybrid coefficients for watermark embedding. Thus, maximum embedding capacity of proposed technique using FRT–DWT is 8 bpp for grayscale image as well as for color images, increasing the embedding capacity 4 times in the proposed technique. Further with direct DWT, the sharp edges in the image will be lost after data hiding. This introduces some loss in the quality of the stego image. This limitation can also be overcome by FRT as it is good at reconstruction of sharp edges.

The rest of the paper is organized as follows; in Section 2, preliminaries used in the design of the proposed technique are given. Section 3 gives the proposed steganography technique, whereas results and discussions are given in Section 4. Finally, the conclusions of the paper are given in Section 5.

2. Preliminaries

In this section, various image processing transforms used in the design of proposed technique are given.

2.1. Finite Ridgelet Transform (FRT)

Donoho [29] introduced the Continuous Ridgelet Transform (CRT) in 2001 as the orientation of 1D wavelet function by constant lines and radial directions. ridgelet transform [30–33] has proved its effectiveness over wavelets. The traditional wavelet transform does not separate smooth information along with edges in the images [33,34]. While wavelet transform represents an image with point singularities, Ridgelet transform represents an image with line singularities. The Finite Ridgelet Transform (FRT) involves two steps: Calculation of Discrete Radon Transform (DRT) followed by application of 1D wavelet transform. Discrete radon transform is also calculated in two steps: Calculation of 2D Fast Fourier Transform (FFT) followed by application of 1D Inverse Fast Fourier Transform (IFFT) on each of the 32 radial directions of the radon projection. The DRT represents the image as a set of projections of different angles in the projection space. For digital images, a projection is calculated by summarization of all data values that lie within specified lines which are defined by finite geometry [35]. The implementation of ridgelet transform depends on the implementation of radon and wavelet transforms [18]. The wavelet transform [36] is applied on each output of radon projection. Finally, the wavelet transform is applied for effective segmentation of point singularity in the Radon domain. Application of FRT on color image involves decomposition of color image is into R, G, and B channels. Then FRT is applied on each channel to get the corresponding ridgelet coefficients. Fig. 1 shows the ridgelet transform coefficients of the image. The main advantage of FRT is that it decomposes any image of size $M \times N$ into its ridgelet transform coefficients of size $2M \times 2N$. This property of FRT is used in the proposed technique to improve embedding capacity of the technique.

Fig. 1. Ridgelet coefficients of color image (a) original color image with size of 256×256 pixels (b) its Ridgelet coefficients with size of 512×512 pixels. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

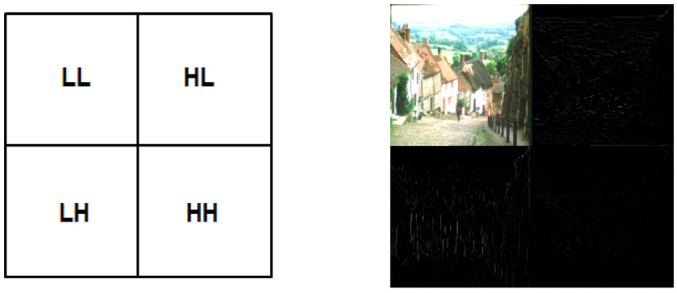


Fig. 2. Wavelet coefficients of color image (a) single level DWT decomposition (b) wavelet coefficients of color image. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

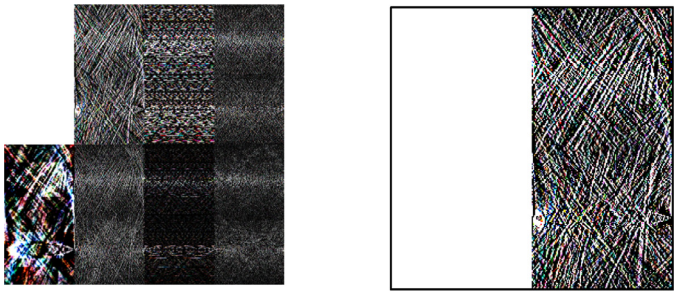


Fig. 3. (a) Hybrid coefficients of color image (wavelet coefficients of Ridgelet coefficients) (b) approximation coefficients of hybrid coefficients of color image. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

2.2. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT) transforms an image into its frequency coefficients. It uses multi resolution where different frequency coefficients are analyzed. The advantage of DWT is that it decomposes an image into two types of coefficients: approximation wavelet coefficients and detail wavelet coefficients. The approximation wavelet coefficients are low frequency coefficients and are denoted as LL subband, whereas detail wavelet coefficients are high frequency coefficients, and are denoted as LH, HL, and HH subband. Fig. 2 shows single level DWT decomposition of color image and its corresponding wavelet coefficients.

In the proposed technique, single level DWT is applied on ridgelet coefficients of cover color image to obtain its hybrid coefficients (wavelet coefficients of ridgelet coefficients). Fig. 3(a) shows

the hybrid coefficients of color image. For secret color image embedding, approximation coefficients (LL subband) of hybrid coefficients of color image which is shown in Fig. 3(b) are used.

2.3. Arnold scrambling

In the proposed steganography technique, Arnold scrambling [28,37] is used to encrypt secret image before embedding it into the cover color image so that attacker cannot extract information of secret image from the stego color image. The resultant chaotic image is secure and cannot be extracted without the knowledge of the scrambling algorithm and secure key. The 2D forward Arnold scrambling is defined by below equation.

$$\begin{vmatrix} i' \\ j' \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \begin{vmatrix} i \\ j \end{vmatrix} \bmod N \tag{1}$$

where, i, j, i', $j' = \{0, 1, 2\ldots N-1\}$; i, j are the pixel coordinates of the original space; i', j' are the pixel coordinates after iterative computation scrambling; N is the size of the secret image. The original secret image is obtained back by inverse Arnold scrambling as follows:

$$\begin{vmatrix} i \\ j \end{vmatrix} = \left(\begin{vmatrix} 2 & -1 \\ -1 & 1 \end{vmatrix} \begin{vmatrix} i' \\ j' \end{vmatrix} + \begin{vmatrix} N \\ N \end{vmatrix} \right) \bmod N \tag{2}$$

3. Proposed steganography technique

In this paper, a color image steganography based on FRT–DWT domains is proposed, in order to make the steganography technique more imperceptible and to support more embedding capacity. In this technique, Arnold scrambling is used to provide security to secret color image before inserting it in the cover color image.

The cover color image to be protected is first divided into R, G, and B channels. The FRT is then applied on each channel values to get ridgelet coefficients of each channel of the cover color image. Following the FRT is single level DWT, which results in a LL, HL, LH and HH subband wavelet coefficients. The LL subband wavelets coefficients are modified according to scrambled secret color image bits and by using an Inserting Factor "IF". A non-blind extraction of secret color image is made possible in proposed technique by using reverse process of inserting process. The block diagram of proposed embedding and extraction processes is given in Fig. 4. The steps involved in secret color image embedding and extraction are given in the following subsections.

3.1. Secret color image embedding process

A scrambled secret color image bit is embedded into FRT–DWT of cover color image using hybrid coefficient values. The algorithm for secret color image embedding is given below:

Step 1. Decompose secret color image into R, G, and B channels.
Step 2. Apply Arnold scrambling on each channel of the secret color image to generate scrambled secret color image in terms of encrypted form.
Step 3. Decompose cover color image into R, G, and B channels.
Step 4. Apply FRT on each channel of cover color image to get ridgelet coefficients of each channel of cover color image.
Step 5. Apply single level DWT on the ridgelet coefficients of each channel to get different wavelet subbands: LL, LH, HL, and HH. Choose the LL subband values for secret color image embedding.
Step 6. Embed each value of encrypted secret color image in LL subband based on the following equations:

$$\begin{aligned} MLL_R &= LL_R + IF \times E_R \\ MLL_G &= LL_G + IF \times E_G \\ MLL_B &= LL_B + IF \times E_B \end{aligned} \tag{3}$$

where, MLL_R, MLL_G, and MLL_B are modified LL subband values of each channel of cover color image; LL_R, LL_G, and LL_B is original LL subband values of each channel of cover color image; IF is inserting Factor; E_R, E_G, and E_B are encrypted values of each channel of secret color image.

Step 7. Apply inverse single level DWT on modified LL subband values with original LH, HL, and HH subband to get modified ridgelet coefficients of each channel of the cover color image.
Step 8. Apply inverse FRT on modified ridgelet coefficients to get modified R–G–B channels of cover color image.
Step 9. Perform image reconstruction on modified R–G–B channel to get a stego color image.

3.2. Secret color image extraction process

In this technique, a scrambled secret color image is extracted non-blindly using the original values of the LL subband of ridgelet coefficients of cover color image and modified values of LL subband of ridgelet coefficients of stego color image. The algorithm for secret color image extraction is given below:

Step 1. Decompose stego color image into R, G, and B channels.
Step 2. Apply FRT on each channel of stego color image to get ridgelet coefficients.
Step 3. Apply single level DWT on the ridgelet coefficients of each channel to get different wavelet subbands: MLL, MLH, MHL, and MHH. The MLL subband values are taken for secret color image extraction.
Step 4. Decompose cover color image into R, G, and B channel.
Step 5. Apply FRT on each channel of cover color image to get ridgelet coefficients of each channel of cover color image.
Step 6. Apply single level DWT on the ridgelet coefficients of each channel to get different wavelet subbands: LL, LH, HL, and HH. Choose LL subband values for secret color image extraction.
Step 7. Extract the scrambled secret color image from stego color image using the following equation:

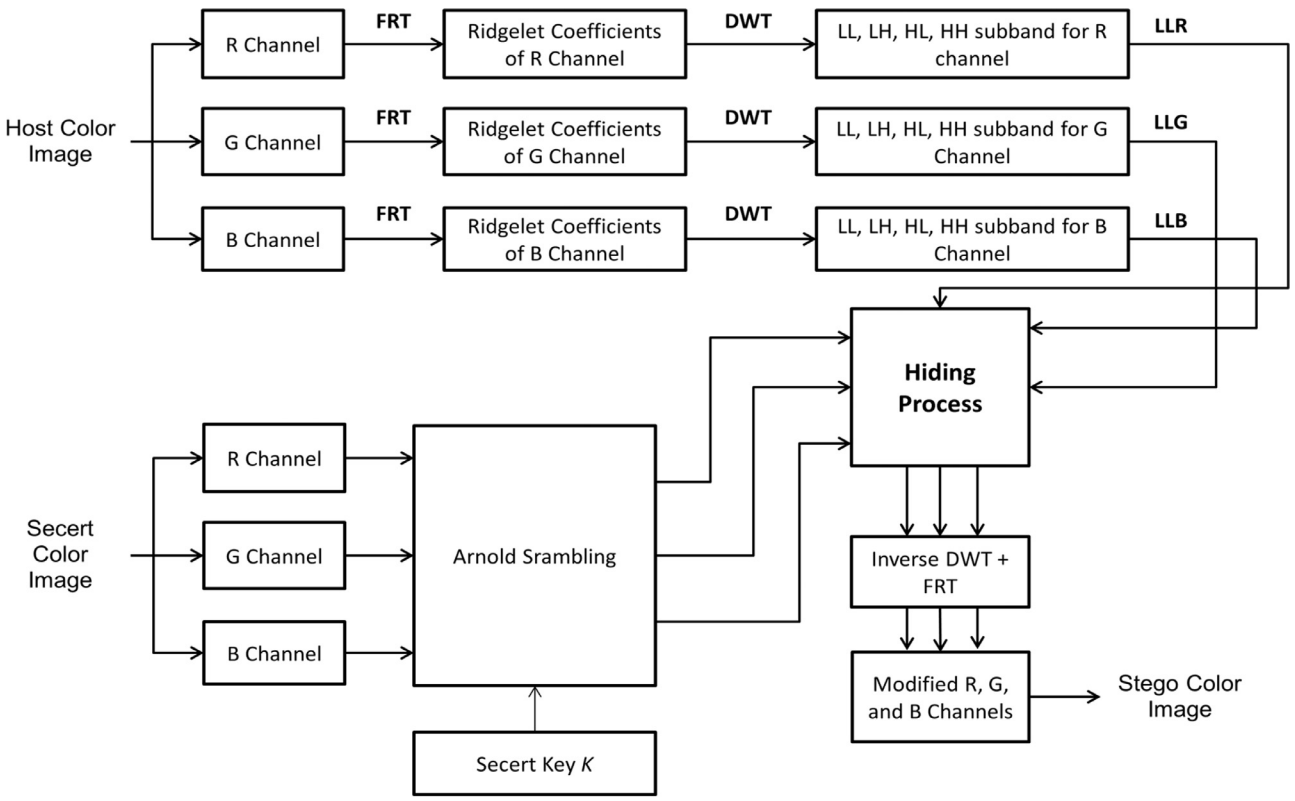
$$\begin{aligned} EE_R &= (MLL_R - LL_R)/IF \\ EE_G &= (MLL_G - LL_G)/IF \\ EE_B &= (MLL_B - LL_B)/IF \end{aligned} \tag{4}$$

Where, MLL_R, MLL_G, and MLL_B are LL subband values of each channel of stego color image; LL_R, LL_G, and LL_B are original LL subband values of each channel of cover color image; IF is inserting factor; EE_R, EE_G, and EE_B are extracted encrypted values of each channel of secret color image.

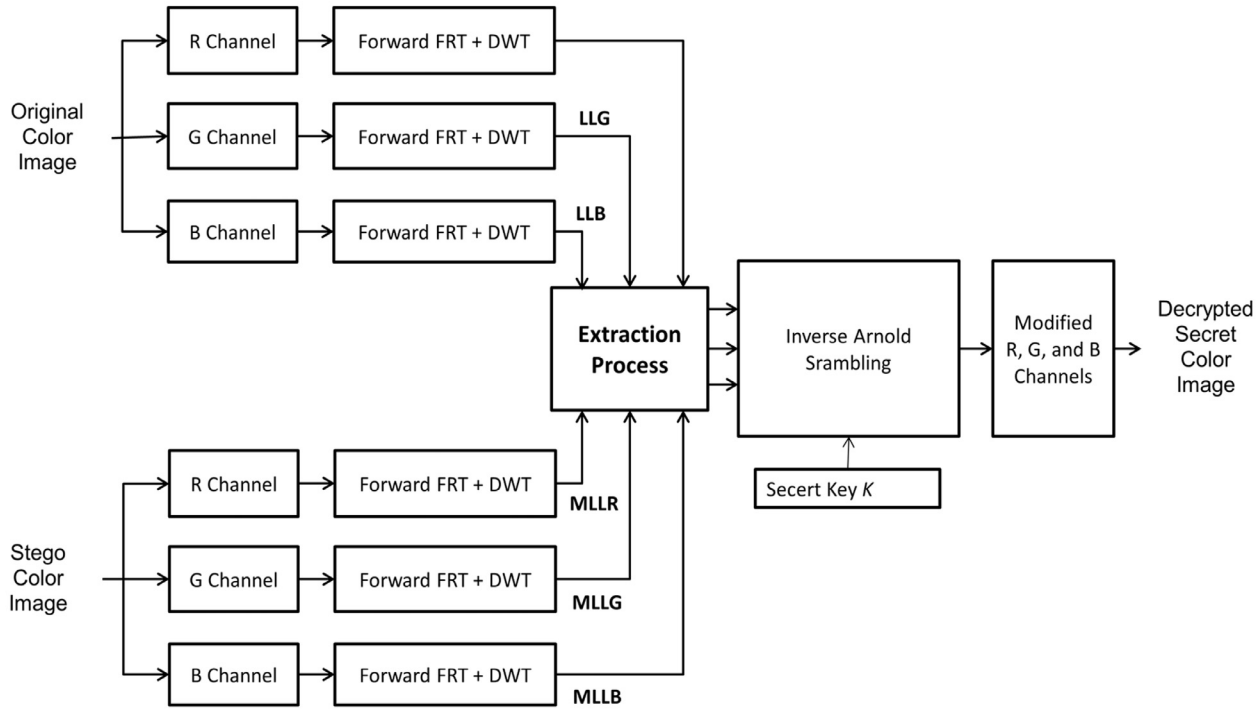
Step 8. Apply inverse Arnold scrambling on each extracted channel values of secret color image to get decrypted values of each channel of secret color image.
Step 9. Perform image reconstruction on decrypted R–G–B channels of secret color image to get decrypted secret color image.

4. Results and discussion

The proposed technique is tested and analyzed on various standard color images such as Lena, Baboon, Barbara, Peppers, Goldhill, Boats and Airplane. These images are taken from The University of South Carolina SIPI Image Database [38], where each image is of size 256×256 pixels with 24 bits. The cover color images are shown in Fig. 5. A color logo is used as secret color image (256×256 pixels) and is shown in Fig. 5(h).



(a)



(b)

Fig. 4. (a) Proposed Secret color image embedding process (b) proposed secret color image extraction process.

Fig. 5. (a) – (g) Test cover color images (h) secret color logo. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

To embed secret color image, each cover color image is divided into R, G, and B channels. Then forward FRT is applied to individual channel to get ridgelet transform coefficients of size 256×256. The single level DWT is applied to ridgelet coefficients to obtain LL, LH, HL, and HH subband for each channel. The LL subband values of each channel are chosen for secret color image embedding. The scrambled secret color image is obtained by applying forward Arnold scrambling on each channel value of secret color image with size 256×256 pixels. Then scrambled secret color image is embedded into the LL subband of cover color image with Inserting Factor (IF). After getting modified LL subband, inverse single level DWT is applied to LL subband with unmodified LH, HL, and HH subbands to obtain modified ridgelet transform coefficients. Then inverse FRT and image reconstruction are applied to these modified ridgelet transform coefficients of each channel of cover color image to get stego color image. For extraction of secret color image from stego color image, first get LL subband of ridgelet coefficients of each channel of stego color image. Then these coefficients values of each channel of stego image are subtracted from corresponding original coefficient values of each channel of cover image, and then results are divided by Inserting Factor (IF) to extract scrambled secret color image. Finally, inverse Arnold scrambling is applied on extracted scrambled watermark to get decrypted secret color image.

4.1. Performance measures

A Peak Signal to Noise Ratio (PSNR) is used to measure imperceptibility between cover color image and stego color image using Eq. (5). A PSNR depends on Mean Square Error (MSE) which is an error between the cover color image and stego color image. The MSE is calculated using Eq. (6). The PSNR is measured in dB; the higher value of PSNR indicates more imperceptibility of the technique.

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \tag{5}$$

$$MSE_R = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(R(x,y) - RS(x,y)\right)^2$$

$$MSE_G = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(G(x,y) - GS(x,y)\right)^2$$

$$MSE_B = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(B(x,y) - BS(x,y)\right)^2$$

$$MSE = \frac{MSE_R + MSE_G + MSE_B}{3} \tag{6}$$

Where, R is the red channel value of cover color image, G is the green channel value of cover color image, B is the blue channel values of cover color image, RS is the red channel value of stego color image, GS is the green channel value of stego color image, and BS is the blue channel values of stego color image. The similarity of the secret color image is measured by Normalized Correlation (NC) [39].

The NC is calculated using Eq. (7). NC measures similarity between the original secret color image and decrypted secret color image. The performance of any steganography technique is high if NC value is near to 1.

$$NC_R = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} S_R(x,y) \times S'_R(x,y)}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} S_R^2(x,y)}$$

$$NC_G = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} S_G(x,y) \times S'_G(x,y)}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} S_G^2(x,y)}$$

$$NC_B = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} S_B(x,y) \times S'_B(x,y)}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} S_B^2(x,y)}$$

$$NC = \frac{NC_R + NC_G + NC_B}{3} \tag{7}$$

Where, S_R is red channel value of secret color image, S_G is green channel value of secret color image, S_B is blue channel value of secret color image, S'_R is red channel value of decrypted secret color

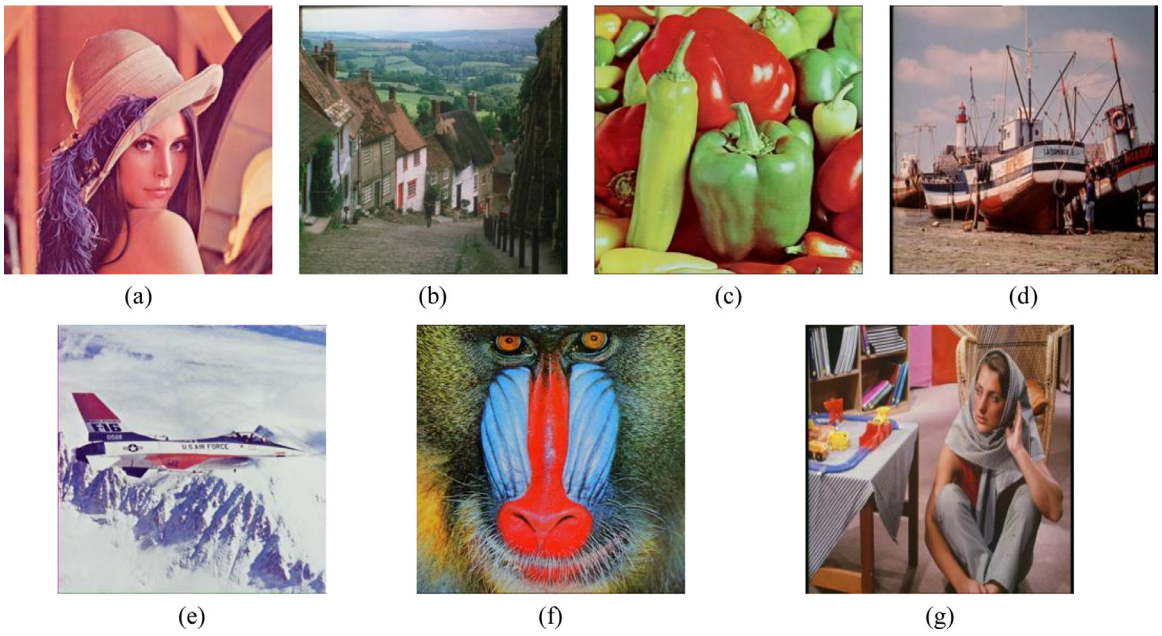


Fig. 6. (a) – (g) Stego color images using IF = 0.2. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

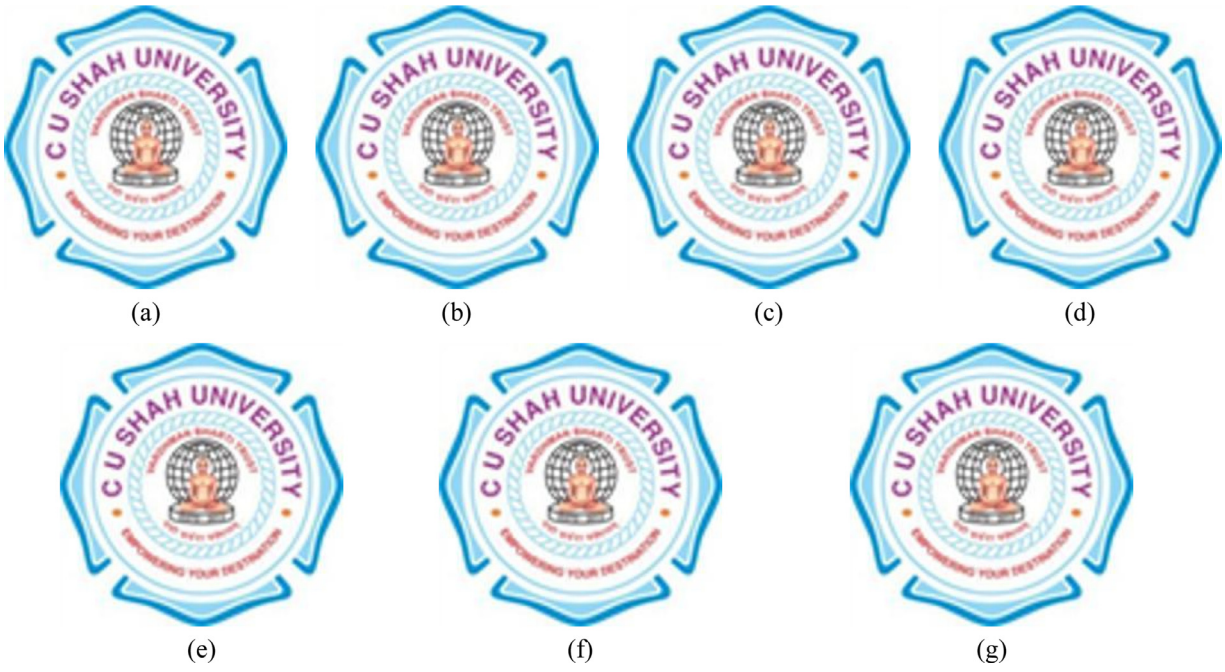


Fig. 7. (a) – (g) Decrypted secret color images using IF = 0.2. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

image, S'_G is green channel value of decrypted secret color image, and S'_B is blue channel value of decrypted secret color image.

4.2. Imperceptibility test

To check the imperceptibility performance of the proposed technique, the secret color image of Fig. 5(h) is embedded in the cover color images of Fig. 5(a) to (g). Fig. 6 shows the set of resultant stego color images after hiding the secret image into them. Results indicate better visual quality. The decrypted secret color images are shown in Fig. 7.

Fig. 8 shows histograms of original cover Lena image, stego Lena image after inserting secret color image using the proposed technique, original secret color image and decrypted secret color image using proposed technique. Fig. 8(a) and (b) are very close in shape indicating that the cover color image is less affected after inserting secret color image in it.

In this technique, Inserting Factor (IF) is used for generation of stego color image. Therefore, various IF values are used for generation of stego color image. The performance of proposed technique is also verified using IF values such as 0.2, 2, and 4. The corresponding PSNR and NC values for the proposed technique are tabulated in Table 1.

The PSNR values being high indicate that the stego image is not noticeably degraded by embedding secret color image in it. The NC values between original secret color image and decrypted secret

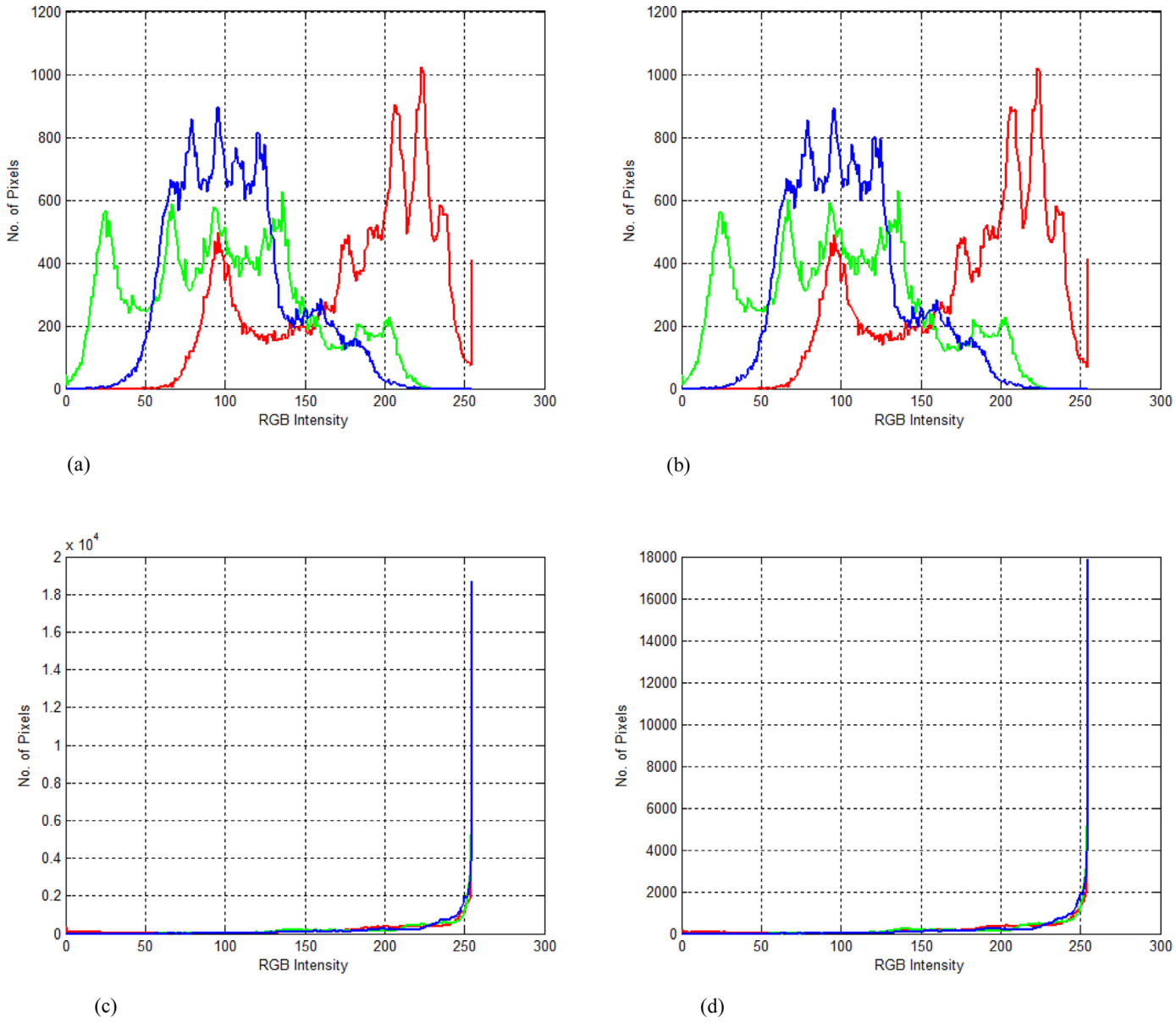


Fig. 8. Histogram of images using proposed steganography approach. (a) Histogram of original cover color lena image. (b) Histogram of stego lena image after inserting secret color image. (c) Histogram of original secret color image. (d) Histogram of decrypted secret color image. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

color image are 1, indicating high quality of decrypted secret image extraction.

4.3. Robustness test

In this section, several benchmark manipulations such as JPEG compression with various quality factors, additional noise (Gaussian, Speckle, and Salt & Pepper), median filtering, mean filtering, histogram equalization, rotation, cropping, sharping and motion blur are applied on stego color image to check the fragile nature of the proposed technique. The Normalized Correlation (NC) values of extracted color secret images when manipulations are applied on stego color image are summarized in Table 2.

Referring the Table 2, the NC values being close to '0′ for all the attacks, the proposed steganography technique has been found fragile and hence can be used to find the data integrity check. The fragility is mainly due to usage of ridgelet frequency coefficients and also the low frequency hybrid coefficients of cover color image for secret image embedding. The low frequency coefficients are directly corrupted when manipulations are applied on stego color image.

Table 1
PSNR (dB) and NC values of stego color image and decrypted color image using different Inserting Factors (IF).

Test Color Image	PSNR (dB)			NC		
	IF = 0.2	IF = 2	IF = 4	IF = 0.2	IF = 2	IF = 4
Lena	58.60	37.84	31.86	1	1	1
Goldhill	59.07	38.21	32.23	1	1	1
Peppers	58.92	38.13	32.15	1	1	1
Boats	58.61	37.85	31.86	1	1	1
Airplane	59.37	38.49	32.50	1	1	1
Baboon	59.02	38.09	32.11	1	1	1
Barbara	58.97	38.14	32.15	1	1	1

Table 2
Fragility performance of the proposed technique for various image processing attacks at IF = 4.

Type of Manipulations	Lena (NC)	Goldhill (NC)	Peppers (NC)	Boats (NC)	Airplane (NC)	Baboon (NC)	Barbara (NC)
JPEG compression (Q = 80)	0.0078	0.00050	0.00068	0.00043	0.0017	0.0017	0.0016
JPEG compression (Q = 70)	0.0075	0.00016	0.00029	0.00003	0.0021	0.0020	0.0017
JPEG compression (Q = 60)	0.0089	0.00007	0.00022	0.00002	0.0023	0.0019	0.0019
JPEG Compression (Q = 50)	0.0115	0.00003	0.00028	0.00008	0.0022	0.0020	0.0018
Gaussian Noise (Mean = 0, Variance = 0.001)	0.0108	0.00035	0.00053	0.00023	0.0020	0.0018	0.0013
Salt & Pepper Noise (Variance = 0.005)	0.0118	0.00031	0.00051	0.00021	0.0019	0.0018	0.0015
Speckle Noise (Variance = 0.005)	0.0114	0.00028	0.00047	0.00024	0.0020	0.0016	0.0014
Median filtering (3 × 3)	0.0128	0.0013	0.0015	0.0013	0.0010	0.00024	0.00014
Average filtering (3 × 3)	0.0156	0.0014	0.0017	0.0014	0.0008	0.00002	0.00047
Histogram equalization	0.0068	0.00084	0.0020	0.0016	0.0077	0.0036	0.0032
Rotation (90°)	0.0022	0.00094	0.0016	0.00088	0.0007	0.0021	0.0028
Cropping	0.0048	0.00045	0.00059	0.0003	0.0017	0.0016	0.0013
Sharping	0.0202	0.0011	0.00080	0.0010	0.0028	0.0035	0.0034
Motion blur	0.0003	0.0021	0.0026	0.0022	0.00006	0.0016	0.0019

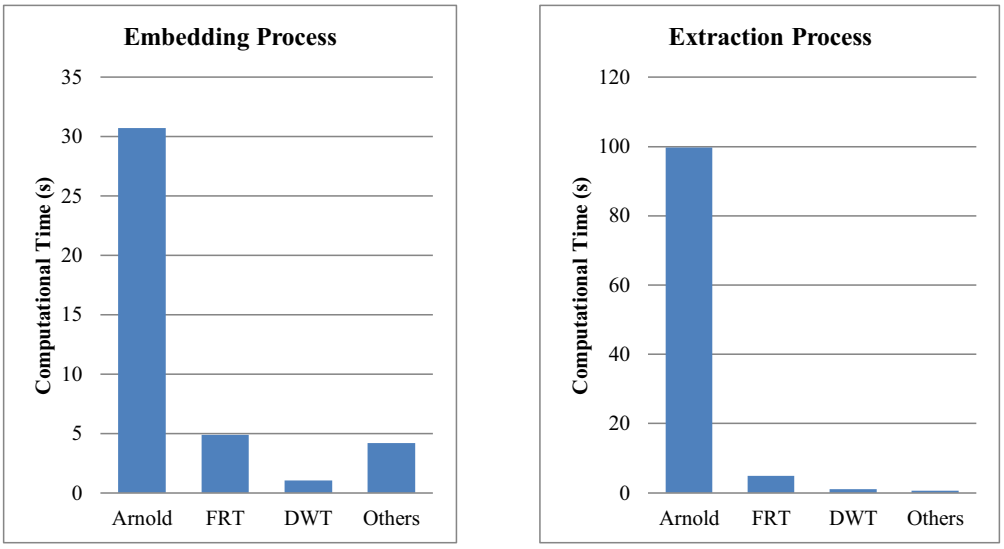


Fig. 9. Computational time (in seconds) of the proposed steganography technique

4.4. Computational complexity

The computational complexity of steganography techniques is usually measured in terms of secret image embedding and extraction processes time. The implementation of the proposed technique is done on the Laptop with 2 GHz core two duo processor with 2GB physical memory using MATLAB 2014a software. In this section, the computational time required for the secret image embedding and extraction processes are calculated using cover Lena image and IF = 0.2. The total computational time for embedding process is 40.811 s and extraction process is 106.321 s, respectively. The computational times of different processes involved are plotted in Fig. 9.

It is to be noted that the steps of Arnold scrambling of secret color image takes almost 90% of the whole computational time. Therefore, the computational time of this step needs to be reduced in future using advanced encryption algorithms and machine with high processing speed and high physical memory in future work.

4.5. Security analysis of proposed technique

In this paper, in order to provide security of secret color image, each channel of secret color image is encrypted by the Arnold scrambling technique with private key k. When the channel value of secret color image is extracted from the stego color image, imposter can't get secret color image without the private key. Hence, the proposed technique has high security. Fig. 10 shows encrypted secret color image generated using forward Arnold scrambling using private key $k = 45$ during inserting process.

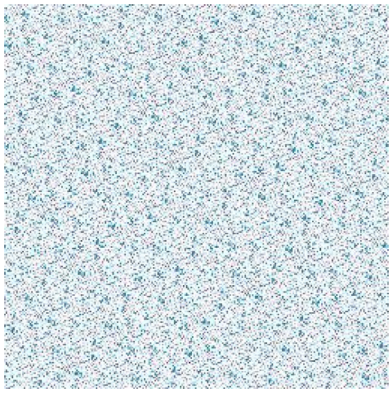


Fig. 10. Encrypted secret color image using private key $k = 45$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

4.6. Hiding capacity analysis of proposed technique

The hiding capacity of steganography technique is defined the number of secret image bits inserted into the cover image and can

Table 3
Comparison of hiding capacity between various techniques.

Steganography technique	Secret color image length (in bits)	Cover color image (in pixels)	Embedding capacity (bits/pixels)
Chou et al. (2003) [20]	$128 \times 128 \times 24$	$512 \times 512 \times 3$	0.50000
Su et al. (2012) [22]	$32 \times 32 \times 24$	$512 \times 512 \times 3$	0.03125
Jia et al. (2017) [28]	$32 \times 32 \times 24$	$512 \times 512 \times 3$	0.03125
Proposed	$256 \times 256 \times 24$	$256 \times 256 \times 3$	8

Table 4
Performance Comparison of Various Techniques.

Test Images	PSNR (dB) for stego color image			
	Liu technique et al., 2017 [40]	Hu technique et al., 2016 [41]	Lin technique et al., 2015 [42]	Proposed technique
Lena	31.84	34.699	31.69	58.60
Goldhill	Not reported	35.493	Not reported	59.07
Peppers	29.99	29.665	29.92	58.92
Airplane	31.12	31.837	31.26	59.37
Baboon	23.58	Not reported	23.61	59.02
Average	29.13	32.92	29.12	58.99

Table 5
Comparison of proposed technique with existing techniques [22,25,26,28] with various features.

Features	Su technique (2012) [22]	Vaishnavi technique (2015) [25]	Rahman technique (2015) [26]	Jia technique (2017) [28]	Proposed technique
Used embedding method	SVD	SVD	DWT+SVD	DWT+QR decomposition	FRT+DWT
Security provided to secret image before inserting	Not provided	Using Arnold scrambling	Not provided	Not provided	Using Arnold scrambling
Maximum PSNR (dB)	39.44	48.34	54.04	41.41	59.37

be calculated using below equation [39]:

$$HC = \frac{Secret\_Bits}{W \times H \times C}(bpp) \tag{8}$$

Where, *HC* is embedding capacity, *Secret_Bits* is total number of bits, *W* is the width of cover image, *H* is the height of cover image, *C* represents number of channels (3 for color image and 1 for grayscale image), and *bpp* is bits per pixel.

In this proposed technique, the total numbers of secret bits are 1,572,864 bits ($256 \times 256 \times 24$) and width as well as height of cover image is 256. Thus, embedding capacity of the proposed technique is calculated as:

$$HC(bpp) = \frac{1572864}{256 \times 256 \times 3} = 8 \tag{9}$$

The hiding capacity of the proposed technique is compared to the related existing techniques in Table 3. Note that the proposed technique has higher hiding capacity than other existing techniques. This is because the proposed technique employs FRT before application of DWT on all channels of cover color image. Recall that the FRT decomposes an image into twice its original size.

4.7. Comparison of proposed technique with existing techniques

In Table 4, the PSNR values of proposed technique are compared with some recent fragile steganography techniques developed for color image authentication. The comparison of techniques is performed by considering the same color images which are used in the proposed technique. The comparison results show that the average PSNR values in Liu technique (2017) [40] is 29.13 dB, Hu technique (2016) [41] is 32.92 dB, Lin technique (2015) [42] is 29.12 dB and in the proposed technique, it is 58.99 dB. This indicates that the proposed technique provides better imperceptibility to stego color image compared to existing steganography techniques.

The proposed steganography technique is compared in respect to various other features in Table 5. The table indicates that the performance of proposed technique is far better in terms of imperceptibility of the stego color image. Further, some of the existing techniques do not encrypt the secret image before hiding. The proposed technique provides better imperceptibility due to its high PSNR value, and high security to secret color image as is encrypted by Arnold scrambling before it is hidden.

5. Conclusions

In this paper, a steganography technique which is based on Finite Ridgelet Transform (FRT), Discrete Wavelet Transform (DWT), and Arnold scrambling is proposed for hiding the secret color image in the cover color image, for the purpose of either securing the secret image in a color image. This is the first paper that employed the FRT to color images security. In this technique, the secret color image is encrypted by Arnold scrambling and then is inserted into the color standard image to a get stego color image. The combination of these three approaches has improved the security of color images over a communication channel. This hybrid technique satisfies all security requirements of color image transmission over a communication channel by allowing high embedding capacity and providing high security to color images. The proposed technique is compared with the existing techniques with respect to various features. It is found from the comparison that the proposed scheme performs better than the existing techniques in terms of imperceptibility and hiding capacity.

Acknowledgments

This research work is funded by the Karnataka Science and Technology Promotion Society, Department of Information Technology, Bio Technology and Science & Technology, Government of Karnataka, India under the category of Seed Money for Young Scientist Research (SMYSR), VGST Scheme.

References

[1] Borra S, Lakshmi H, Dey N, Ashour A, Shi F. Digital image watermarking tools: state-of-the-art. Front Artif Intell Appl 2017;296:450–9.
[2] Ashour A, Dey N. Security of multimedia contents: a brief. Intell Tech Signal Process Multimedia Secur 2017:3–14.
[3] Borra S, Swamy G. Sensitive digital image watermarking for copyright protection. In: Int *J Netw Secur*, 15; 2013. p. 95–103.
[4] Borra S, Swamy G. A spatial domain public image watermarking. Int J Secur Appl 2011;5(1):1–11.
[5] Phadikar A, Verma B, Jain S. Region splitting approach to robust color image watermarking scheme in wavelet domain. Asian J Inf Manage 2007;1(2):27–42.
[6] Anitha J, Pandian S. A color image digital watermarking scheme based on SOFM. Int J Comput Sci Issues 2010;7(5):302–9.
[7] Gunjal B. Wavelet based color image watermarking scheme giving high robustness and exact correlation. Int J Emerging Trends Eng Technol 2011;1(1):21–30.
[8] Dey N, Pal M, Das A. A session based blind watermarking technique within the NROI of retinal fundus images for authentication using DWT, Spread Spectrum, and Harris corner detection. Int J Mod Eng Res 2012;2(3):749–57.
[9] Eswaraiah R, Reddy E. Robust watermarking method for color images using DCT coefficients of watermark. Global J Comput Sci Technol 2012;12(2) (1).
[10] Gunjal B, Mail S. Strongly robust and highly secured DWT–SVD based color image watermarking: embedding data in all Y, U, V color spaces. Int J Inf Technol Comput Sci 2012;3:1–7.
[11] Liu G, Liu H, Kadir A. Wavelet based color pathological image watermark dynamically adjusting the embedding intensity. Comput Math Methods Med 2012 2012.
[12] Nasir I, Abdurrman A. A robust color image watermarking scheme based on image normalization. In: Proceedings of the world congress on engineering 2013, 3; 2013.
[13] Yan H, Yang W. A watermarking algorithm based on wavelet and Hadamard transform for color image. J Software Eng Appl 2013;6:58–61.
[14] ElGamal A, Mosa N, ElSaid W. Block-based watermarking for color images using DCT and DWT. Int J Comput Appl 2013;66(15):33–40.
[15] Shi H, Fangliang L, Cao Y. A blind watermarking technique for color image based on SVD with circulation. J Software 2014;9(7):1749–56.
[16] Deshmukh S, Bhatia S, Talwar R. Blind watermarking scheme based on RDWT-DCT for color images. Int J Tech Res Appl 2014;2(4):117–21.
[17] Rahman M, Rabbi M. DWT-SVD based new watermarking idea in RGB color space. Int J Signal Process Image Process Pattern Recognit 2015;8(6):193–8.
[18] Shakunthala B, Naveen N, Shresta S, Bharathi P, Manjunath D, Pooja B. A Perception based color image adaptive watermarking scheme in YCbCr SPAC. Int J Emerging Res Manage Technol 2017;6(2):108–18.
[19] Abraham J, Paul V. An imperceptible spatial domain color image watermarking scheme. J King Saud Univ Comput Inf Sci 2017. DOIhttp://dx.doi.org/10.1016/j.jksuci.2016.12.004.
[20] Chou C, Wu T. Embedding color watermarks in color images. EURASIP J Appl Signal Process 2003;2003(1):32–40.
[21] Biswas D, Biswas S, Sarkar P, Sarkar D, Banerjee S, Pal A. Comparison and analysis of watermarking algorithms in color images – image security paradigm. Int J Comput Sci Inf Technol 2011;3(3):33–47.
[22] Su Q, Niu Y, Liu X, Zhu Y. Embedding color watermarks in color images based on Schur decomposition. Opt Commun 2012;285:1792–802.
[23] Su Q, Wang G, Jia S, Zhang X, Liu Q, Liu X. Embedding color image watermark in color image based on two-level DCT. Signal Image Video Process 2015;9(5):991–1007.
[24] Kumar A, Anuradha. A novel watermarking algorithm for color images based on Discrete Wavelet Transform. Int J Comput Electr Eng 2014;6(4):303–6.
[25] Vaishnavi D, Subashini T. Robust and invisible image watermarking in RGB color space using SVD. Procedia Comput Sci 2015;46:1770–7.
[26] Rahman M, Rabbi M. Non-blind DWT–SVD based watermarking technique for RGB image. Global J Res Eng 2015;15(4).
[27] Freitas P, Farias M, Araujo A. Hiding color watermarks in halftone images using maximum similarity binary patterns. Signal Process 2016;48:1–11.
[28] Jia S, Zhou Q, Zhou H. A novel color image watermarking scheme based on DWT and QR decomposition. J Appl Sci Eng 2017;20(2):193–200.
[29] Donoho D. Ridge functions and orthonormal ridgelets. J Approximation Theory 2001;111(2):143–79.
[30] Do M, Vetterli M. Orthonormal finite ridgelet transform for image compression. In: Proceedings of the international conference on image processing, (ICIP '00); 2000. p. 367–70.
[31] Candes E, Donoho D. A surprisingly effective non-adaptive representation for objects with edges, curves and surfaces. Nashville, USA: Vanderbilt University Press; 2000.
[32] Candes E. Ridgelets theory and application Ph.D. Thesis. Department of Statistics, Stanford University; 1998.
[33] AlZubi S, Islam N, Abbod M. Multiresolution analysis using wavelet, ridgelet, and curvelet transforms for medical image segmentation. Int J Biomed Imaging 2011:4 2011.
[34] Candes E, Donoho D. Ridgelets: a key to higher dimensional intermittency? Philos Trans R Soc A 1999;357(1760):2495–509.
[35] He J. A characterization of inverse Radon transform on the Laguerre hypergroup. J Math Anal Appl 2006;318(1):387–95.
[36] Dettori L, Semler L. A comparison of wavelet, ridgelet and curvelet-based texture classification algorithms in computed tomography. Comput Biol Med 2007;37(4):486–98.
[37] Roy S, Pal A. A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. Multimedia Tools Appl 2017;76(3):3577–616.
[38] The university of south carolina SIPI image database: http://sipi.usc.edu/database/database.php.
[39] Kutter M, Petitcolas F. A fair benchmark for image watermarking systems. Electronic imaging'99. Secur Watermarking Multimedia Contents 1999;3657:1–14.
[40] Liu XL, Lin CC, Lin CH, Lin LJ, Qiu BJ. Reversible authentication scheme for demosaicked images without false detection. In: Advances in intelligent information hiding and multimedia signal processing: proceeding of the twelfth international conference on intelligent information hiding and multimedia signal processing, November 21–23, 2016, 1. Springer International Publishing; 2017. p. 313–20.
[41] Hu YC, Lo CC, Chen WL. Probability-based reversible image authentication scheme for image demosaicking. Future Gener Comput Syst 2016;62:92–103.
[42] Lin CC, Lin CH, Liu XL, Yuan SM. Fragile watermarking-based authentication scheme for demosaicked images. In: Intelligent information hiding and multimedia signal processing (IIH-MSP), 2015 international conference on. IEEE; 2015. p. 97–100.
[43] Hussain M, Wahab AWA, Ho AT, Javed N, Jung KH. A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Process 2017;50:44–57.
[44] Hussain M, Wahab AWA, Javed N, Jung KH. Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Tech Rev 2016:1–11.
[45] Hussain M, Abdul Wahab AW, Javed N, Jung KH. Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. Symmetry 2016;8(6):41.